Watermarking Method Resistant to Geometrical Slight Distortion Using Variance of Color Difference and Wavelet Transform

Kei Sakiyama[1a], Motoi Iwata[1], Akio Ogihara[1] and Akira Shiozaki[1]
[1]Graduate School of Engineering, Osaka Pefecture University
1-1 Gakuen-cho, Naka-ku, Sakai, Osaka, 599-8531, Japan E-mail : [a]sakiyama@ch.cs.osakafu-u.ac.jp

Abstract: In this paper, we propose a watermarking method that has robustness against geometrical slight distortions. The method is based on the variances of two color components of an image. We use YCbCr components. When an image is geometrically distorted, Cb and Cr components on the same position cause the same distortion, and the relation of variances of Cb and Cr components in a local domain does not change easily. So we embed a watermark by changing the variances of Cb and Cr components so that the watermark may be robust against geometrical distortions. Moreover we use discrete wavelet transform so as to be robust against JPEG compression.

1. Introduction

Various digital watermarking methods that are robust against JPEG compression and noise addition attacks have been proposed. But the digital watermarking methods that are robust against geometrical distortion have not been developed yet.

A watermark method that embeds a watermark in specific positions has to specify embedded positions when the watermark is extracted. But the embedded positions attacked by geometrical distortion may shift. Then, we cannot specify the embedded positions and cannot extract the watermark. Alghoniemy et al. [1] proposed two watermarking methods that are robust against geometrical distortions. One method uses the invariant moments of an image that are robust against geometrical distrotions, and another method uses the normalization of an original image. There is a watermarking method that is robust against geometrical ditortion using feature points of an original image [2]. But the methods in [1][2] only detect whether a specific bit pattern is embedded or not. Luo et al. [3] proposed a watermarking method based on inherent features of an image that are geometrically invariant. The method can embed and extract a multibit watermark, but the robustness against geometrical distortion is not enough yet. Dong et al. [4] proposed two watermarking methods that are robust against geometrical distortions. One method uses the normalization of an original image, and another method is based on mesh modeling. Both methods employ a direct-spread code division multiple access (DS-CDMA) approach to embed a multibit watermark in the discrete cosine transform domain of an image and are robust against geometrical distortion and JPEG compression. But the quality of the watermarked images has not been estimated. A digital watermarking method using two color components has been proposed [5]. The method can embed and extract an arbitrary bit pattern. But it is not robust against JPEG compression though it is robust against geometrical distortion.

In this paper, we propose a digital watermarking method that can embed and extract an arbitrary bit pattern and is robust against geometrical slight distortion and JPEG compression. The proposed method do not need the original image when the emebedded watermark is extracted.

When an image is geometrically distorted, Cb and Cr components on the same positon cause the same distortion. So, the relation of variances of Cb and Cr components in a local domain does not change easily. Using this behavior, we embed a watermark by changing the variances of Cb and Cr components. It also uses discrete wavelet transform (DWT) so as to be robust against JPEG compression.

In this paper, Section 2 describes the proposed method. In Section 3, we present experimental results. Section 4 describes discussion and Section 5 concludes the paper.

2. The Proposed Method

2.1 Embedding Method

We explain embedding process. Let a watermark be $W = \{w_l | w_l \in \{0,1\}, 0 \leq l < L\}$. Let I denote an original color image with $X \times Y$ pixels. I is transformed to wavelet coefficients using two dimensional descrete wavelet transform (DWT). The LL subband of the wavelet coefficients is expressed in YCbCr color spaces. Let Cb and Cr denote Cb components and Cr components of LL subband. We divide Cb and Cr into blocks $Cb_{(i,j)}$ and $Cr_{(i,j)}$ of size $N \times N$ $(0 \leq i < X/2N,\ 0 \leq j < Y/2N)$. One bit of a watermark is embedded by changing variances of $K = \lfloor (X/2N \times Y/2N)/L \rfloor$ blocks selected at random without duplication. We save the information on embedded positions as a secret key. Let T denote embedding strength, and let $Cb^{(l,k)}$ and $Cr^{(l,k)}$ $(0 \leq k < K)$ respectively denote K blocks of Cb and Cr, where w_l is embedded. Let $Cb^{(l,k)}(x_b, y_b)$ and $Cr^{(l,k)}(x_b, y_b)$ respectively denote the values of the coordinate (x_b, y_b) in $Cb^{(l,k)}$ and $Cr^{(l,k)}$ $(0 \leq x_b < N,\ 0 \leq y_b < N)$. Let $V(Cb^{(l,k)})$ and $V(Cr^{(l,k)})$ respectively denote the variances of $Cb^{(l,k)}$ and $Cr^{(l,k)}$. Embedding is performed by changing $Cb^{(l,k)}$ and $Cr^{(l,k)}$ to $Cb'^{(l,k)}$ and $Cr'^{(l,k)}$ using Eqs.(1)-(4) according to w_l.

- if $w_l = 1$ and $V(Cb^{(l,k)}) - V(Cr^{(l,k)}) < T$, then

$$\begin{cases} \left.\begin{array}{l} V(Cb'^{(l,k)}) = P^{(l,k)} \\ V(Cr'^{(l,k)}) = Q^{(l,k)} \end{array}\right\} & \text{if } \mathrm{Q}^{(\mathrm{l,k})} \geq 0 \\ \left.\begin{array}{l} V(Cb'^{(l,k)}) = T \\ V(Cr'^{(l,k)}) = 0 \end{array}\right\} & \text{if } \mathrm{Q}^{(\mathrm{l,k})} < 0 \end{cases} \quad (1)$$

- if $w_l = 0$ and $V(Cr^{(l,k)}) - V(Cb^{(l,k)}) < T$, then

$$\begin{cases} \left.\begin{array}{l} V(Cb'^{(l,k)}) = Q^{(l,k)} \\ V(Cr'^{(l,k)}) = P^{(l,k)} \end{array}\right\} & \text{if } \mathrm{Q}^{(\mathrm{l,k})} \geq 0 \\ \left.\begin{array}{l} V(Cb'^{(l,k)}) = 0 \\ V(Cr'^{(l,k)}) = T \end{array}\right\} & \text{if } \mathrm{Q}^{(\mathrm{l,k})} < 0 \end{cases} \tag{2}$$

where

$P^{(l,k)} = \frac{V(Cb^{(l,k)})+V(Cr^{(l,k)})}{2} + \frac{T}{2}$,

$Q^{(l,k)} = \frac{V(Cb^{(l,k)})+V(Cr^{(l,k)})}{2} - \frac{T}{2}$.

$Cb'_{(l,k)}(x_b, y_b) =$

$$\begin{cases} \sqrt{\frac{V(Cb'^{(l,k)})}{V(Cb^{(l,k)})}}(Cb^{(l,k)}(x_b, y_b) - \overline{Cb^{(l,k)}}) + \overline{Cb^{(l,k)}} \\ \qquad\qquad \text{if } V(Cb^{(l,k)}) \neq 0 \\ (-1)^{(x_b+y_b)}\sqrt{V(Cb'^{(l,k)})} + Cb^{(l,k)}(x_b, y_b) \\ \qquad\qquad \text{if } V(Cb^{(l,k)}) = 0 \end{cases} \tag{3}$$

$Cr'_{(l,k)}(x_b, y_b) =$

$$\begin{cases} \sqrt{\frac{V(Cr'^{(l,k)})}{V(Cr^{(l,k)})}}(Cr^{(l,k)}(x_b, y_b) - \overline{Cr^{(l,k)}}) + \overline{Cr^{(l,k)}} \\ \qquad\qquad \text{if } V(Cr^{(l,k)}) \neq 0 \\ (-1)^{(x_b+y_b)}\sqrt{V(Cr'^{(l,k)})} + Cr^{(l,k)}(x_b, y_b) \\ \qquad\qquad \text{if } V(Cr^{(l,k)}) = 0 \end{cases} \tag{4}$$

where $\overline{Cb^{(l,k)}}$ and $\overline{Cr^{(l,k)}}$ denote the average values of $Cb^{(l,k)}$ and $Cr^{(l,k)}$. After embedding process, YCbCr color components of blocks are changed to RGB color components. Then we get the watermarked image I' by inverse discrete wavelet transform. But the pixel values of I' may overflow or underflow by embedding a watermark. As a result, the difference of $V(Cb'^{(l,k)})$ and $V(Cr'^{(l,k)})$ may become smaller than T. Then we culculate the least upper bounds (LUB) and the greatest lower bounds (GLB) of $Cb'^{(l,k)}(x_b, y_b)$ and $Cr'^{(l,k)}(x_b, y_b)$ for the pixel values to enter in the range. But the LUB and the GLB of a color component cannot be culculated unless the value of another color component is decided. So we first culculate the LUB and the GLB of the color component that belongs to the block whose variance will be decreased, and change the values of the color component so as to be within the bounds. Next we culculate the LUB and the GLB of another color component and change the values of the color component so as to be within the bounds. Thus we repeatedly performe embedding process until the difference of $V(Cb')$ and $V(Cr')$ become T or more. We omit the detalis because of limited space.

2.2 Extraction Method

Extraction method is as follows. A watermarked image I' is transformed to wavelet coefficients by DWT. We get $Cb'^{(l,k)}$ and $Cr'^{(l,k)}$ in the same way as embedding by using the secret key. Then we get a watermark by Eq. (5)

$$\begin{cases} w_l = 1 & \text{if } \rho_l \geq 0 \\ w_l = 0 & \text{if } \rho_l < 0 \end{cases} \tag{5}$$

where $\rho_l = \sum_{k=0}^{K-1}\{V(Cb'^{(l,k)}) - V(Cr'^{(l,k)})\}$.

Table 1. T and PSNR

Original Image	T	PSNR[dB]
Aerial	90	32.3
Airplane	60	32.1
Earth	70	32.2
Lena	80	32.4
Mandrill	90	32.3
Milkdrop	20	32.3
Pepper	20	32.3
Sailboat	70	32.0

3. Experiment

3.1 Experimetal Condition

Original images are eight color images with 256 × 256 pixels and 256 brightness level for RGB color components, which are “Aerial,” ”Airplane,” “Earth,” ”Lena,” ”Mandrill,” ”Milkdrop,” “Pepper” and “Sailboat”. The block size N is 8. We used ten random bit sequences of 64 bits as ten watermarks. Under the above conditions, K is equal to 4. We attacked watermarked images using StirMark4.0 [6][7] and investigated the robustness of the prposed method. “Removelines,” “Rescale,” “Rotation” and “JPEG Compression” were used in StirMark4.0. “Removelines” removes some rows and colummns of an image and the parameter r means that $\lfloor X/r \rfloor$ columns and $\lfloor Y/r \rfloor$ rows are removed. “Rescale” changes an image size and the parameter means the percentage of the changed size, where the original image size is 100. “Rotation” rotates an image and the parameter means the angle (degree) of left-rotation. For watermarked images attacked by “Removelines” and “Rescale”, we resampled them to the original images size using IrfanView32(ver3.99)[1] and then extracted the watermark. For watermarked images attacked by “Rotation”, we resized them to the original images size by cutting away the margin and then extracted the watermark. We used PSNR[dB] to evaluate the watermarked image quality. We adjusted embedding strength T so that PSNR may be nearly equal to 32[dB]. Table 1 shows T and PSNR for each image. We defined the correct extraction rate (CER) for evaluating the robustness of the proposed method as follows:

$$\mathrm{CER} = \frac{\text{the number of correctly extracted bits}}{\text{the number of embedded bits}} \times 100[\%]. \tag{6}$$

[1] http://www.irfanview.com/

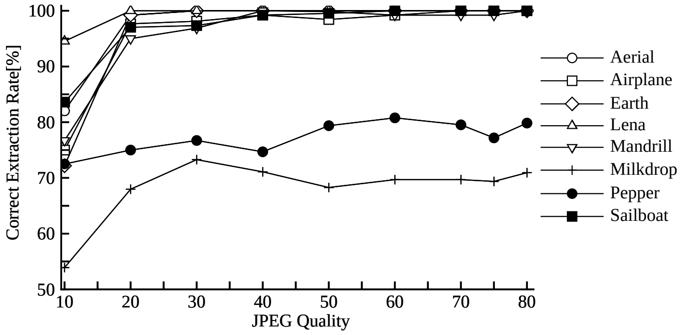

Figure 1. CER versus JPEG quality

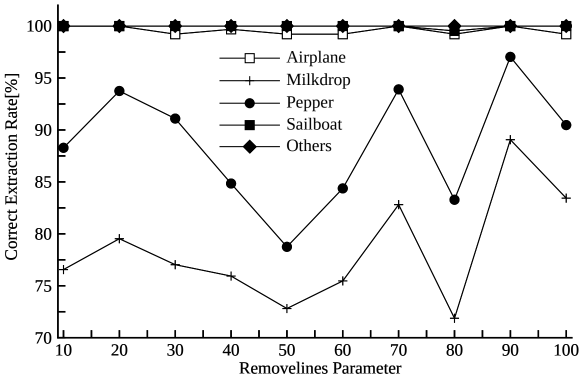

Figure 2. CER for “Removelines”

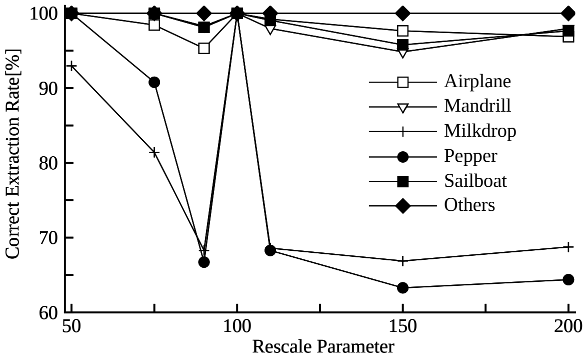

Figure 3. CER for “Rescale”

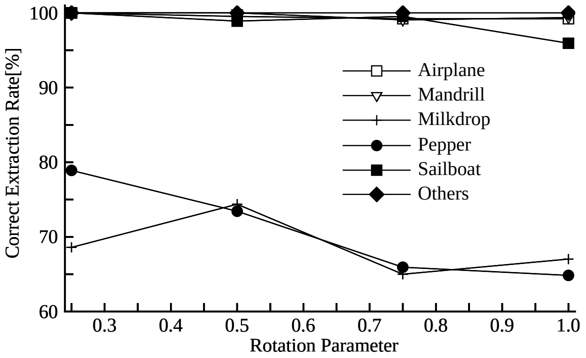

Figure 4. CER for “Rotation”

3.2 Experimental Results

The CERs shown in Fig.1–4 are the average values of those of ten watermarks. Figure 1 shows the experimental results for JPEG compression. For JPEG compression, “Aerial”, “Earth” and “Lena” maintained the CERs of 100% when JPEG quality was from 30 to 80. “Airplane”, “Mandrill” and “Sailboat” maintained the CERs over 95% when JPEG quality was from 20 to 80. But “Milkdrop” and “Pepper” did not maintain the CERs over 80 % for all JPEG quality.

Figure2–4 show the experimental results for “Removelines”, “Rescale” and “Rotation” respectively. For “Removelines”, “Aerial”, “Earth”, “Lena” and “Mandrill” maintained the CERs of 100% for all parameters, and “Airplane” and “Sailboat” maintained the CERs of over 99% for all parameters. But the CER of “Pepper” became less than 80% when the parameter was 50, and the CER of “Milkdrop” did not maintain over 90% for all parameters. For “Rescale”, “Aerial”, “Earth” and “Lena” maintained the CERs of 100% for all parameters, and “Airplane”, “Mandrill” and “Sailboat” maintained the CERs over 94% for all parameters. But “Milkdrop” and “Pepper” did not maintain the CERs of 70% when the parameter was 90, 110, 150 and 200. For “Rotation”, “Aerial”, “Earth” and “Lena” maintained the CERs of 100% for all parameters, and “Airplane”, “Mandrill” and “Sailboat” maintained the CERs over 95% for all parameters. But “Milkdrop” and “Pepper” did not maintain the CERs of 80% for all parameters.

For all attacks, the CERs of “Milkdrop” and “Pepper” were lower than those of the other images.

4. Discussion

Watermarking methods in [1][2] are robust against gemetrical distortions, but these methods only specify whether the watermark is embedded or not, and do not specify a bit pattern of extracted watermark. On the other hand, the proposed method can specify a bit pattern of extracted watermark. Watermarking methods in [3][4][5] specify a bit pattern of extacted watermark. The method in [3] embeds a watermark by using the inherent features of an image that are geometrically invariant, but the robustness against geometrical distortion is enough yet. Though the method in [4] is robust against geometrical distortions and JPEG compression, it embedds only 50 bits and the quality of watermarked images is unknown. The method in [5] embeds a watermark by using the covariance of two color components. The method is robust against geometrical distortion for only two images, and cannot keep the CER over 90% for JPEG compression of quality 75. The proposed method keeps the CER over 90% for “JPEG compression” of quality from 30 to 80 for six images among eight images.

In the proposed method, for images where the difference of the variances of Cb and Cr components is large, like “Mikldrop” and “Pepper”, the change of the pixel values by embedding a watermark is apt to become large. So we could not make the embedding strength high to maintain PSNR at nearly 32[dB], and so the robustness of the watermarked images became low. The proposed method embeds a watermark by multiplying the values of Cb and Cr components in each block by each magnification ratio. The larger the absolute value of a component is, the larger the amount of change becomes. When the large absolute value of the components in a block is shifted by geometrical distortion, the variance of the block changes largely. Then the watermark cannot be extracted correctly from the block. So the robustness of each block against attacks differs, and it depends on not only embedding strength T but the values of Cb and Cr components in the block. The degradation of watermarked images that consist of the complicated domains is hard to perceive, but the degradation of the flat domains is easy to perceive. The proposed method is effective in a color image with many complicated domains. Though we evaluated the robustness against “JPEG compression”, “Removelines”, “Rescale” and “Rotation”, we need to evaluate the robustness against other attacks.

5. Conclusion

In this paper, we proposed a digital watermarking method that is robust against geometrical distortion. The proposed method embeds a watermark by changing the variances of Cb and Cr components of a color image. The method also has robustness against JPEG compression by using DWT. The method do not need an original image when an embedded watermark is extracted. Most of the methods that are robust against geometrical distortion specify whether a watermark is embedded or not, while the proposed method can embed and extract an arbitrary bit pattern. The proposed method is more effective in a color image with many complicated domains.

References

[1] M.Alghoniemy and A.H.Tewfik, “Geometric invariance in image watermarking,” *IEEE Trans. Image processing*, vol.13, no.2, pp.145-153, 2004.

[2] P.Bas, J.M.Chassery, and B.Macq, “Geometrically invariant watermarking using feature points,” *IEEE Trans. Image Processing*, vol.11, no.9, pp.1014–1028, 2002

[3] J.Luo and H.wang, “Connectivity-based image watermarking,” *IEICE Trans. Fundamentals.*, vol.E89-A, no.4, pp1126–1128, 2006

[4] P.Dong, J.G.Brankov, N.P.Galatsanos, Y.Yang, and F.Davoine, “Digital watermarking robust to geometric distortions,” *IEEE Trans. Image Processing*, vol.14, no.12, pp.2140–2150, 2005

[5] H.Yoshiura and I.Echizen, “Color picture watermarking correlating two constituent planes for immunity to random geometric distortion,” *IEICE Trans.Inf. & Syst.*, vol.E87-D, no.9, pp.2239–2252, 2004

[6] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, “Attacks on copyright marking systems,” *Information Hiding: Second International Workshop*. LNCS 1525, Springer-Verlag, pp. 219–239, 1998

[7] F. A. P. Petitcolas, “Watermarking schemes evaluation,” *IEEE Trans. Signal Processing*, vol. 17, no. 5, pp. 58–64, 2000.